## REMARKS

In this Amendment, Applicant has cancelled Claim 4 without prejudice or disclaimer and amended Claims 1 – 3 to specify the embodiments of the present invention and overcome the pending rejections. It is respectfully submitted that no new matter has been introduced by the amended claims. All claims are now present for examination and favorable reconsideration is respectfully requested in view of the preceding amendments and the following comments.

REJECTIONS UNDER 35 U.S.C. § 102:

Claim 1 has been rejected under 35 U.S.C. § 102 (e) as allegedly being anticipated by Den Boer et al. (US 6,298,136), hereinafter Den Boer.

Applicant traverses the rejection and respectfully submits that the present-claimed invention is not anticipated by the cited reference. More specifically, the embodiment of the present invention as defined in the amended Claim 1 includes the feature of "prior to carrying out said two-place operation on i-th subblock and subkey, a substitution operation is performed on the subkey depending on j-th subblock, where $i \neq j$." Such feature is not disclosed or taught by Den Boer.

The amended claims reciting the specific type of operation of subkey conversion depending on data subblocks which was not previously known in the prior art. This specific type of operation is a substitution operation performed on a subkey depending on one of data subblocks. Claim 1 recites, instead of a conversion operation of a general type performed on the subkey, the specific type of the conversion operation. Such conversion operation is a substitution operation performed on the subkey depending on the data being converted. The feature of converting the subkey using the substitution operation depending on the data being converted is not disclosed or suggested by Den Boer. The term "substitution operation" introduced in the amended Claim1 is disclosed in the specification, in particular, in the original Claim 4.

Applicant respectfully direct the Examiner's attention to the fact that the operation of permuting subkey bits recited in amended Claim 2 is a special case of the substitution operation indicated in Claim 1 and the operation of cyclic offsetting subkey bits recited in amended Claim 3 is a specific case of the operation of permuting indicated in Claim 2.

It is respectfully submitted that Den Boer discloses a feature of converting subkeys using the operation of permuting bits. However, the operation of permuting subkey bits mentioned in Den Boer **does not depend on any of data subblocks being converted**. In particular, this is clear from the fact that at different values of the input data block, the same cyclic offsetting operation is performed on the data (see Fig.3 and column 2, lines 1-15). According to Den Boer, the operation of converting the subkeys may be performed **in advance** prior to any data block entering the input of the encryption algorithm. Therefore, the subkeys are converted using the cyclic offsetting operation which **does not depend on any data subblock**.

With regards to Fig.6 and Fig.7 cited by the Examiner, it is clear from the text of the specification relating to these figures (lines 12-37) that the subkeys are part of the function of converting data subblocks, which can be considered as a two-place operation performed on the subblock and the subkey. Because, prior to performing this operation, the subkeys are not subject to any conversion depending on any data subblock, Den Boer lacks any feature of performing an operation on the subkey depending on the data subblock. The presence of such feature in the claimed invention (performing the substitution operation on the subkey depending on the subblock) constitutes an important difference from Den Boer and from other known methods of data block encryption.

Therefore, the newly presented claim is not anticipated by Den Boer and the rejection under 35 U.S.C. § 102 (e) has been overcome. Accordingly, withdrawal of the rejection under 35 U.S.C. § 102 (e) is respectfully requested.

REJECTIONS UNDER 35 U.S.C. § 103:

Claims 2 – 4 have been rejected under 35 U.S.C. § 103 as allegedly being unpatentable over by Den Boer, in view of Coppersmith et al. (US 6,192,129), hereinafter Coppersmith.

Applicant traverses the rejection and respectfully submits that the embodiments of present-claimed invention are not obvious over Den Boer, in view of Coppersmith. Claim 4 has been cancelled. Therefore, the rejection to Claim 4 is moot. As stated above, Den Boer does not disclose the invention as amended. Similarly, Coppersmith also fails to teach or suggest the embodiments of the present invention as defined in Claims 2 – 3.

The embodiment of the present invention as amended includes a new feature that consists in dependency of the substitution operation (in a particular case, the operation of permuting subkey bits) performed on the subkey, on one of the data subblocks being converted. The aggregate of the feature of performing the substitution operation (in a special case, permuting bits or cyclic offsetting) and the feature of depending on the operation performed on a subkey on a data subblock being converted is **novel and non-obvious**. In particular, this solution has been confirmed as being novel and significant in the following published research work:

1. Moldovyan A.A., Moldovyan N.A. A cipher based on data-dependent permutations. Journal of Cryptology, 2002, No. 1. pp. 61—72;
2. Goots N.D., Moldovyan A.A., Moldovyan N.A. Fast encryption algorithm SPECTR-H64 // Proceedings of the International workshop, Methods, Models and Architectures for Network Security / Lect. Notes Comput. Sci., Berlin: Springer-Verlag, 2001, vol. 2052, pp. 275-286
3. N. Sklavos, and O. Koufopavlou, "Data Dependent Rotations, a Trustworthy Approach for Future Encryption Systems/Ciphers: Low Cost and High Performance", Computers and Security, Elsevier Science Journal, Vol. 22, No. 7, 2003.

4. Youngdai Ko, Deukjo Hong, Seokhie Hong, Sangjin Lee, Jongin Lim: Linear Cryptanalysis on SPECTR-H64 with Higher Order Differential Property, Int. Workshop MMM-ANCS 2003, Proc. LNCS, Springer-Verlag, Berlin, 2003, vol. 2776, pp. 298-307.

As we previously pointed out, in Coppersmith, round subkeys are generated according to a determined law. Therefore, during the encryption of various data blocks, the value of subkeys remains unchanged over a preset conversion step of some preset round in the encryption methods described in Coppersmith. In addition, as admitted by the Examiner, Den Boer does not expressly disclose either an operation of permuting subkey bits or a substitute operation performed on a subkey as being the conversion operation step. Therefore, there is no motivation to combine Den Boer and Coppersmith. Even if they are combined, Den Boer and Coppersmith will not render the present claimed invention obvious. One of ordinary skill in the art would not discern the present invention as claimed at the time of its invention.

Therefore, the newly presented claims are not anticipated by Den Boer and Coppersmith and the rejection under 35 U.S.C. § 103 has been overcome. Accordingly, withdrawal of the rejections under 35 U.S.C. § 103 is respectfully requested.

Having overcome all outstanding grounds of rejection, the application is now in condition for allowance, and prompt action toward that end is respectfully solicited.

Respectfully submitted,

JACOBSON HOLMAN PLLC

Date: September 19, 2005
(202) 638-6666
400 Seventh Street, N.W.
Washington, D.C. 20004
Atty. Dkt. No.: P65855US0

By _____
John C. Holman
Registration No. 22,769